R E P U B L I Q U E F R A N Ç A I S E

09/889362 #5
PCT/FR 99/02918

FIO

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

FR 99/02918

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA REGLE 17.1.a) OU b)

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 02 DEC. 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

SIEGE
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 14/1/99

N° D'ENREGISTREMENT NATIONAL 99 00341

DÉPARTEMENT DE DÉPÔT 75

DATE DE DÉPÔT 14 JAN. 1999

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Cabinet BALLOT-SCHMIT
16, avenue du Pont Royal
94230 Cachan

n°du pouvoir permanent / références du correspondant: n° 014365 — téléphone: 01.49.69.91.91

2 DEMANDE Nature du titre de propriété industrielle

X brevet d'invention ☐ demande divisionnaire

certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé X immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui X non

Titre de l'invention (200 caractères maximum)

Procédé cryptographique à clés publique et privée

3 DEMANDEUR (S) n° SIREN . . . . . code APE-NAF . . . .

Nom et prénoms (souligner le nom patronymique) ou dénomination

GEMPLUS

Forme juridique

S.C.A.
(Société en commandite par Actions)

Nationalité (s) Française

Adresse (s) complète (s) — Pays

Avenue du Pic de Bertagne
Parc d'activités de la Plaine de Jouques
13420 GEMENOS

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☐ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt : joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine | numéro | date de dépôt | nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

BORIN Lydie
Mandataire n° 94-0506
Cabinet BALLOT-SCHMIT

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION — SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

BA 540 A/7100*04

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

BREVET D'INVENTION CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL
9900341

n° 014365

TITRE DE L'INVENTION :

Procédé cryptographique à clés publique et privée

LE(S) SOUSSIGNÉ(S)

BORIN Lydie
Cabinet BALLOT-SCHMIT
16, avenue du Pont Royal
94230 Cachan

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

- PAILLIER Pascal

domicilié : Cabinet BALLOT-SCHMIT
16, avenue du Pont Royal
94230 Cachan

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Cachan, le 13 janvier 1999

BORIN Lydie
Mandataire n° 94-0506
Cabinet BALLOT-SCHMIT

BA 113/140897

DOCUMENT COMPORTANT DES MODIFICATIONS

PAGE(S) DE LA DESCRIPTION OU DES REVENDICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
6, 13, 14, 25,				13/07/1993	SA - 11 AOUT 1993
26, 28, 32				et 05/28/1993	

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifées).

PROCEDE CRYPTOGRAPHIQUE A CLES PUBLIQUE ET PRIVEE

La présente invention concerne un procédé cryptographique à clés publique et privée. Il est utilisable dans toutes les applications dans lesquelles il est nécessaire d'assurer la confidentialité des messages transmis sur un canal quelconque et/ou d'identifier avec certitude un dispositif avec lequel on échange des messages.

La confidentialité de messages transmis entre deux dispositifs A et B sur un canal de communication quelconque est obtenue en chiffrant l'information transmise pour la rendre inintelligible aux personnes à qui elle n'est pas destinée. L'identification certaine d'un dispositif est lui basé le calcul de la signature numérique d'un message.

En pratique, deux types de procédé cryptographique peuvent être utilisés celui dit symétrique, à clés secrètes, dont un exemple bien connu est le DES...celui dit asymétrique, utilisant une paire de clés publique et privée et décrit dans « *New directions in Cryptography* » *IEEE Transactions on Information Theory, nov. 1976, par* MM Diffie et Hellman. Un exemple bien connu de procédé asymétrique est le RSA, du nom de ses inventeurs Ronald Rivest, Adi Shamir et Léonard Adleman. On peut trouver une description de ce procédé RSA dans le brevet américain US 4, 405, 829.

Dans l'invention, on s'intéresse plus particulièrement à un procédé cryptographique asymétrique.

Un procédé de chiffrement selon un procédé cryptographique asymétrique consiste principalement, pour un émetteur A qui veut envoyer confidentiellement un message à un destinataire B à prendre connaissance, par exemple dans un annuaire, de la clé publique K_B du destinataire B, à appliquer le procédé de chiffrement E sur le message m à transmettre en utilisant cette clé publique, et à envoyer au destinataire B, le cryptogramme c résultant: $c= E_{KB}(m)$.

Ce procédé consiste principalement pour le destinataire B, à recevoir le cryptogramme c, et à le déchiffrer pour obtenir le message d'origine m, en appliquant le procédé de déchiffrement D sur le cryptogramme c en utilisant la clé privée K'b qu'il est le seul à connaître: m=Dk'b(c).

Selon ce procédé n'importe qui peut envoyer un message chiffré au destinataire B, mais seul ce dernier est capable de le déchiffrer.

On utilise habituellement un procédé cryptographique asymétrique pour la génération/vérification de signature. Dans ce contexte, un utilisateur qui veut prouver son identité utilise une clé privée, connue de lui seul, pour produire une signature numérique s d'un message m, signature qu'il transmet au dispositif destinataire. Ce dernier met en oeuvre la vérification de la signature en utilisant la clé publique de l'utilisateur. Tout dispositif a ainsi la capacité de vérifier la signature d'un utilisateur, en prenant connaissance de la clé publique de cet utilisateur et en l'appliquant dans l'algorithme de vérification. Mais seul l'utilisateur concerné a la capacité

de générer la bonne signature utilisant sa clé privée. Ce procédé est par exemple beaucoup utilisé dans les systèmes de contrôle d'accès ou de transactions bancaires. Il est en général couplé à l'utilisation d'un procédé de chiffrement, pour chiffrer la signature avant de la transmettre.

Pour cette génération/vérification de signatures numériques, on peut utiliser en pratique des procédés cryptographiques asymétriques dédiés à cette application, tel le DSA *(Digital Signature Algorithm)*, qui correspond à un standard américain proposé par le *US National Institute of Standards and Technology*. On peut en outre utiliser le RSA qui a la propriété de pouvoir être utilisé aussi bien en chiffrement qu'en génération de signature.

Dans l'invention, on s'intéresse à un procédé cryptographique qui peut être utilisé pour le chiffrement des messages et pour la génération de signature numérique. Dans l'état actuel de la technique, seul le RSA, dont il existe de nombreuses variantes de mise en oeuvre, offre cette double fonctionnalité.

Le RSA comprend une étape de génération des clés publique K et privée K' pour un dispositif donné dans laquelle on procède de la façon suivante :

- on choisit deux grands nombres premiers p et q, distincts.
- on calcule leur produit n=p.q.
- on choisit un nombre e premier avec le plus petit commun multiple de (p-1)(q-1). En pratique, e est souvent pris égal à 3.

La clé publique K est alors formée par le couple de paramètres (n,e) et la clé secrète K' est formée par le couple de paramètres (p,q).

En choisissant p et q de grande taille, leur produit n est aussi de grande taille. N est donc très difficile à factoriser : on est assuré que l'on ne pourra pas retrouver la clé secrète K'=(p,q) à partir de la connaissance de n .

Le procédé de chiffrement d'un nombre m représentant un message M, $0 \leq m < n$ consiste alors, à effectuer le calcul suivant :

$c = E_B(m) = m^e \bmod n$

au moyen de la clé publique K=(n,e).

Le procédé de déchiffrement consiste lui dans le calcul inverse suivant :

$m = c^d \bmod (n)$

au moyen de la clé privée K'=(p,q), gardée secrète, où

$$d = \frac{1}{e} \bmod (p-1)(q-1).$$

On a vu que le RSA a la particularité d'être utilisable pour la vérification de signature. Le procédé correspondant de génération de signature par un utilisateur A consiste à utiliser le procédé de déchiffrement avec la clé secrète pour produire la signature s d'un nombre m représentatif d'un message. On a ainsi : $s = m^d \bmod n$.

Cette signature s est transmise à un destinataire B. Ce dernier, qui connaît m (par exemple, A transmet s et m), vérifie la signature en effectuant l'opération inverse, c'est à dire en utilisant le procédé de chiffrement avec la clé

publique de l'émetteur A. C'est à dire qu'il calcule $v=s^e \bmod n$, et vérifie $v=m$.

En général, pour améliorer la sécurité d'un tel procédé de vérification de signature, on applique préalablement une fonction de hachage sur le nombre m avant de calculer la signature, qui peut consister en des permutations de bits et/ou une compression.

Quand on parle de message M à chiffrer ou à signer, il s'agit bien sûr de messages numériques, qui peuvent résulter d'un codage numérique préalable. Ce sont en pratique des chaînes de bits, dont la taille binaire (nombre de bits) peut être variable.

Or un procédé de cryptographie comme le RSA est tel qu'il permet de chiffrer avec la clé publique (n,e) n'importe quel nombre entre 0 et n-1. Pour l'appliquer à un message M de taille quelconque, il faut donc en pratique couper ce message en une suite de nombres m qui vérifieront chacun la condition $0 \leq m < n$. On applique alors le procédé de chiffrement sur chacun de ces nombres. Dans la suite, on s'intéresse donc à l'application du procédé cryptographique sur un nombre m représentatif du message M. m peut-être égal à M, ou en n'être qu'une partie. On désigne alors indifféremment dans la suite par m le message ou un nombre représentatif du message.

Un objet de l'invention, est un procédé de cryptographie asymétrique différent de ceux basés sur le RSA.

Un objet de l'invention, est un procédé reposant sur d'autres propriétés, qui puisse s'appliquer aussi bien en chiffrement de messages qu'en génération de signatures.

Un objet de l'invention, est un procédé de cryptographie qui permette, dans certaines configurations, un temps de traitement plus rapide.

Telle que caractérisée, l'invention concerne un procédé cryptographique selon la revendication 1.

L'invention sera mieux comprise à la lecture de la description suivante , faite à titre indicatif et nullement limitatif de l'invention et en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma fonctionnel d'un système de communication cryptographique de type asymétrique;
- la figure 2 est un schéma fonctionnel d'un dispositif communiquant utilisé dans un système de communication cryptographique selon l'invention;
- la figure 3 est un organigramme d'une session de chiffrement/déchiffrement de messages utilisant le procédé cryptographique selon l'invention; et
- la figure 4 est un organigramme d'une session de génération/vérification de signature utilisant le procédé cryptographique selon l'invention.

Pour bien comprendre l'invention, il est nécessaire de faire quelques préliminaires mathématiques.

Dans la description, on utilise les notations mathématiques suivantes :

(1) Si a est un entier relatif et b un entier strictement positif, a mod b (a modulo b) est le résidu modulaire de a relativement à b et désigne l'unique entier strictement inférieur à b tel que b divise (a - a mod b).

(2) (Z/bZ) désigne l'ensemble des résidus modulo b et forme un groupe pour l'addition modulaire .

(3) $(Z/bZ)^*$ désigne l'ensemble des entiers inversibles modulo b et forme un groupe pour la multiplication modulaire.

(4) L'ordre d'un élément a de $(Z/bZ)^*$ est le plus petit entier naturel ord(a,b) tel que $a^{ord(a,b)}=1 \bmod b$.

(5) PPCM (a,b) désigne le plus petit commun multiple de a et b.

(6)PGCD(a,b) désigne le plus grand commun diviseur de a et b.

(7) $\lambda(a)$désigne la fonction de Carmichael de a. Si $a=p.q$, $\lambda(a)=PPCM(p-1, q-1)$.

(8) On note $x=TRC(a_1,...a_k, b_1,...b_k)$ l'unique solution, obtenue par la mise en oeuvre du Théorème du Reste Chinois bien connu, du système d'équations modulaires suivant :

$x=a_1 \bmod b_1$

$x= a_2 \bmod b_2$

...

$x= a_k \bmod b_k$.

où les entiers a_i et b_i sont donnés et où, $\forall i,j$ avec $i\neq j$, $PGCD(bi, b_j)=1$.

(9) On rappelle que la taille binaire d'un nombre a est le nombre de bits sur lesquels a s'écrit.

Soit maintenant un nombre n, entier, de taille arbitraire. L'ensemble $Un=\{x<n^2 / x=1 \bmod n\}$ est un sous-groupe multiplicatif de $(Z/n^2Z)^*$.

Soit alors $\log_n$ la fonction définie sur l'ensemble Un par :

$$\log_n(x) = \frac{x-1}{n}$$

Cette fonction a la propriété suivante :

$\forall\ x \in Un,\ \forall\ y \in Un,\ \log_n(xy \bmod n^2) = \log_n(x) + \log_n(y) \bmod n$.

Par conséquent, si g est un nombre entier arbitraire appartenant à Un, on a pour tout nombre m, $0 \leq m < n$:

$\log_n(g^m \bmod n^2) = m.\log_n(g) \bmod n$.

Cette propriété mathématique est à la base du procédé de cryptographie mis en oeuvre dans l'invention qui va maintenant être décrite.

La figure 1 représente un système de communication cryptographique, utilisant un procédé cryptographique asymétrique. Il comprend des dispositifs communiquants, dans l'exemple A et B, sur un canal de communication 1. Dans l'exemple, on a représenté un canal bidirectionnel. Chaque dispositif contient une paire de clés publique K et privée K'.

Les clés publiques sont par exemple publiées dans un fichier public 2 tel qu'un annuaire, que chaque dispositif peut consulter. Dans ce fichier public, on trouvera ainsi la clé publique K_A du dispositif A et celle K_B du dispositif B.

La clé privée K' de chaque dispositif est conservée par lui de façon secrète, typiquement dans une zone sécurisée de mémoire non volatile. Le dispositif A contient ainsi en mémoire secrète sa clé privée K'_A et le dispositif B contient ainsi en mémoire secrète sa clé privée K'_B. Ils

conservent aussi leur clé publique, mais dans une zone mémoire sans protection d'accès particulière.

Dans un tel système, le dispositif A peut chiffrer un message m en un cryptogramme c_A en utilisant la clé publique K_B du dispositif B; ce dernier peut déchiffrer c_A en utilisant sa clé privée K'_B, qu'il conserve secrètement. Inversement, , le dispositif B peut chiffrer un message m en un cryptogramme c_B en utilisant la clé publique K_A du dispositif A; ce dernier peut déchiffrer c_B en utilisant sa clé privée K'_A, qu'il conserve secrètement.

Typiquement, chaque dispositif comprend au moins, comme représenté sur la figure 2, des moyens de traitement 10, c'est à dire une unité centrale de traitement (CPU), comprenant notamment différents registres R pour le calcul, une interface de communication 11 avec le canal de communication, et des moyens de mémorisation. Ces moyens de mémorisation comprennent généralement une mémoire programme 12 (ROM, EPROM, EEPROM) et une mémoire de travail (RAM) 13 . En pratique, chaque dispositif conserve ses données secrètes dans une zone d'accès sécurisée 120 prévue en mémoire programme et ses données publiques dans une zone d'accès normal de cette mémoire. La mémoire de travail permet de conserver momentanément, le temps nécessaire aux calculs, des messages à chiffrer, des cryptogrammes à déchiffrer, ou encore des résultats de calculs intermédiaires.

Les moyens de traitement et de mémorisation permettent ainsi d'exécuter des programmes liés à l'application, et notamment d'effectuer les calculs correspondant à la mise en oeuvre du procédé de

cryptographie pour le chiffrement /déchiffrement de messages et/ou la génération/vérification de signatures selon l'invention. Ces calculs comprennent notamment, comme on le verra de façon détaillée dans la suite, des élévations à la puissance, des résidus et inversions modulaires .

Les dispositifs peuvent encore comprendre un générateur 14 de nombre aléatoire ou pseudo-aléatoire r , qui peut intervenir dans les calculs précités, dans certaines variantes de réalisation. Ce générateur est encadré en pointillé sur la figure 2, pour indiquer qu'il n'est pas nécessaire à la réalisation de toutes les variantes de réalisation selon l'invention.

Tous ces moyens du dispositif sont connectés à un bus d'adresses et de données 15.

De tels dispositifs utilisés dans l'invention sont bien connus, et correspondent par exemple à ceux qui sont utilisés dans les systèmes de communication cryptographique de l'état de la technique, mettant en oeuvre le RSA. Ils ne seront donc pas détaillés plus avant. Un exemple pratique de système de communication cryptographique, est le système formé des serveurs bancaires et des cartes à puce, pour la gestion de transactions financières. Mais il existe de nombreuses autres applications, telle les applications liées au commerce électronique .

Un premier mode de réalisation de l'invention va maintenant être détaillé, au regard de l'organigramme représenté sur la figure 3.

Cet organigramme représente une séquence de communication entre un dispositif A et un dispositif B sur un canal de communication 20. Ces dispositifs comprennent au moins les moyens de traitement, de mémorisation et de communication décrits en relation avec la figure 2.

Le procédé de cryptographie selon l'invention comprend un procédé de générations des clés publique K et privée K'.

Selon l'invention, ce procédé de génération des clés publique et privée d'un dispositif comprend les étapes suivantes :

- sélection de deux grands nombres premiers p et q distincts et de taille voisine;
- calcul du nombre n égal au produit p.q;
- calcul du nombre $\lambda(n)=PPCM(p-1 , q-1)$, c'est à dire de la fonction de Carmichael du nombre n;
- détermination d'un nombre g, $0 \leq g < n^2$, qui remplisse les deux conditions suivantes :

a) g est inversible modulo n^2 et

b) $ord(g,n^2)=0 \bmod n$.

Cette condition b) indique que l'ordre du nombre g dans l'ensemble $(Z/n^2Z)^*$ des nombres entiers de 0 à n^2 est un multiple non nul du nombre n, selon les notations définies plus haut.

La clé publique K est alors formée par le nombre n et le nombre g. La clé privée est formée par les nombres p,q et $\lambda(n)$ ou seulement par les nombres p et q, $\lambda(n)$ pouvant être recalculé à chaque utilisation de la clé secrète.

On génère selon ce procédé les clés publique et privée de chaque dispositif. Cette génération peut-être effectuée, selon les dispositifs considérés et les applications, par les dispositifs eux-mêmes ou par un organe externe.

Chaque dispositif, par exemple le dispositif A, contient donc en mémoire sa clé publique $K_A = (n_A, g_A)$ et, de façon secrète, sa clé privée $K'_A = (p_A, q_A)$.

En outre, les clés publiques sont mises dans un fichier accessible au public.

On verra ci-dessous qu'il est avantageux de choisir $g=2$, lorsque c'est possible, c'est à dire, lorsque $g=2$ remplit les conditions a) et b) du procédé de génération de signature selon l'invention.

Un procédé de chiffrement selon un premier mode de réalisation du procédé cryptographique de l'invention mis en oeuvre dans le dispositif A consiste alors, pour l'envoi d'un message au dispositif B, dans la réalisation des étapes suivantes, avec $0 \leq m < n$:

- renseignement des paramètres n et g du procédé de chiffrement mis en oeuvre par le dispositif A par la clé publique K_B du deuxième dispositif B : $n = n_B$, $g = g_B$.
- calcul du cryptogramme $c = g^m \bmod n^2$, et
- transmission du cryptogramme c sur le canal de communication.

Le procédé de chiffrement selon un premier mode de réalisation de l'invention consiste donc à prendre le paramètre g de la clé publique, à l'élever à la puissance m, et à calculer le résidu modulaire relativement à n^2. On

notera que dans le RSA, c'est le message m qui est élevé à la puissance alors que dans l'invention, le message m est utilisé comme exposant.

Le dispositif B qui reçoit le message chiffré, c'est à dire le cryptogramme c, met alors en oeuvre un procédé de déchiffrement selon l'invention avec les paramètres de sa clé privée. Ce procédé de déchiffrement comprend le calcul suivant :

- calcul du nombre m tel que

$$m = \frac{\log_n(c^{\lambda(n)} \bmod n^2)}{\log_n(g^{\lambda(n)} \bmod n^2)} \bmod n$$

où

$$\log_n(x) \quad \frac{x-1}{n} .$$

Si g=2, on voit que le calcul d'élévation de g à la puissance est facilité. On prendra donc de préférence g=2, toutes les fois où ce sera possible. En d'autres termes, le procédé de génération des clés commencera par essayer si g=2 remplit les conditions a) et b).

Différentes variantes de calcul du procédé de déchiffrement peuvent être mises en oeuvre, qui permettent, lorsque le dispositif doit déchiffrer un grand nombre de cryptogrammes, de précalculer certaines quantités et de les conserver de façon secrète dans le dispositif. Une contrepartie est que la zone mémoire secrète (zone 120 sur la figure 2) du dispositif doit être plus étendue, puisqu'elle doit alors contenir des paramètres supplémentaires en plus des paramètres p et q. Ceci n'est pas sans influencer le choix de mise en oeuvre d'une variante ou d'une autre. En effet, la réalisation

d'une zone de mémoire sécurisée est coûteuse, et donc de capacité (mémoire) généralement limitée, notamment dans les dispositifs dits à bas côuts (par exemple, certains types de cartes à puce).

Dans une première variante de mise en oeuvre du procédé de déchiffrement, on prévoit que le dispositif, B en l'occurrence, précalcule une fois pour toutes la quantité :

$$\alpha_{n,g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

et la conserve secrète en mémoire.

Ainsi, on réduit d'autant le temps nécessaire au déchiffrement de chacun des messages reçus par le dispositif. En effet, lorsque que le dispositif B exécute une instance de cette variante du procédé de déchiffrement, il ne lui reste plus qu'à calculer :

$$m = \log_n(c^{\lambda(n)} \bmod n^2)\ \alpha_{n,g} \bmod n.$$

Dans une deuxième variante de mise en oeuvre du procédé de déchiffrement selon l'invention, on prévoit d'utiliser le Théorème du Reste Chinois, pour une meilleure efficacité (rapidité du calcul).

Dans une instance de cette deuxième variante du procédé de déchiffrement, le dispositif effectue les calculs (de déchiffrement) suivants :

1 $m_p = \log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

2 $m_q = \log_q(c^{q-1} \bmod q^2)\log_p(g^{q-1} \bmod q^2)^{-1} \bmod q$

3 $m = TRC(m_p, m_q, p, q)$,

où

$$\log_p(x) \quad \frac{x-1}{p} \qquad \text{et}$$

$$\log_q(x) \quad \frac{x-1}{q}$$

Dans ce cas, on peut en outre prévoir, dans les cas où le dispositif est amené à déchiffrer un très grand nombre de messages, que le dispositif précalcule une fois pour toutes les quantités suivantes :

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$ et

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$.

Le dispositif doit alors conserver ces quantités comme données secrètes.

Le calcul effectué lors d'une instance du procédé de déchiffrement devient :

1. $m_p = \log_p(c^{p-1} \bmod p^2)\ \alpha_{p,g} \bmod p$
2. $m_q = \log_q(c^{q-1} \bmod q^2)\ \alpha_{q,g} \bmod q$
3. $m = TRC(m_p, m_q, p, q)$.

Comme déjà précisé, toutes ses variantes de calcul de déchiffrement sont intéressantes lorsque le dispositif est amené à déchiffrer un très grand nombre de messages, et que le gain en temps de traitement compense la plus grande capacité mémoire de la zone sécurisée pour conserver toutes les données secrètes. Le choix de l'une ou l'autre variante dépend en pratique de l'application considérée et des contraintes de coûts et de temps de traitement à concilier.

Un deuxième mode de réalisation de l'invention comprend l'utilisation d'un nombre aléatoire, fournit par un générateur de nombre aléatoire (ou pseudo-aléatoire), dans le procédé de chiffrement, en sorte que pour un même message m à transmettre, le cryptogramme calculé c sera

différent à chaque fois. La sécurité du système de communication est donc plus grande. Le procédé de déchiffrement est inchangé.

Ce deuxième mode de réalisation de l'invention comprend deux variantes.

Dans une première variante, le cryptogramme c est obtenu par le calcul suivant : $c=g^{m+nr} \bmod n^2$.

Dans une deuxième variante, le cryptogramme c est obtenu par le calcul suivant : $c=g^m r^n \bmod n^2$.

Cette deuxième variante nécessite en pratique un temps de traitement plus long que la première, mais elle offre une plus grande sécurité.

Dans un troisième mode de réalisation de l'invention, on impose que l'ordre de g dans $(Z/nZ)^*$ soit un entier de petite taille, ceci étant obtenu par une mise en oeuvre du procédé de génération des clés différente.

Avec une telle condition sur l'ordre du paramètre g, on réduit la complexité du calcul du procédé de déchiffrement qui devient en pratique quadratique (c'est à dire en x^2) par rapport à la taille du nombre n.

Dans ce troisième mode de réalisation de l'invention, le procédé de génération des clés publique et privée est alors le suivant :

- sélection en secret, d'un entier u et de deux grands nombres premiers p et q distincts et de taille voisine tels que u divise (p-1) et divise (q-1).
- calcul du nombre n égal au produit p.q;
- calcul du nombre $\lambda(n)=PPCM(p-1 , q-1)$, c'est à dire de la fonction de Carmichael du nombre n;

- détermination d'un nombre h, $0 \leq h < n^2$, qui remplisse les deux conditions suivantes :

a) h est inversible modulo n^2 et

b) $ord(h,n^2) = 0 \bmod n$.

- calcul du nombre $g = h^{\lambda(n)/u} \bmod n^2$.

La clé publique K est alors formée par le nombre n et le nombre g. La clé privée est constituée par les entiers (p,q,u) conservés secrètement dans le dispositif.

De préférence, on choisit h=2, lorsque c'est possible (c'est à dire si h=2 remplit les conditions a) et b), pour faciliter le calcul de g.

On notera que si u =PGCD(p-1,q-1), il n'est pas nécessaire de conserver ce nombre qui peut-être retrouvé par le dispositif à partir de p et q.

De préférence, on choisira u premier, pour améliorer la sécurité du procédé, et de petite taille, typiquement 160 bits. En choisissant une petite taille pour u, on verra que l'on facilite le calcul de déchiffrement.

Dans ce troisième mode de réalisation, la mise en oeuvre du procédé de chiffrement pour chiffrer un message m est identique à celle précédemment décrite dans le premier mode de réalisation de l'invention, le cryptogramme étant égal à $c = g^m \bmod n^2$.

On peut aussi calculer le cryptogramme c en utilisant une variable aléatoire r selon la première variante du deuxième mode de réalisation de l'invention précédemment décrit. r est alors un entier aléatoire, de même taille que u et le cryptogramme est obtenu par le calcul suivant : $c = g^{m+nr} \bmod n^2$.

Le cryptogramme c calculé selon l'une ou l'autre mise en oeuvre précédente du procédé de chiffrement est envoyé au dispositif B qui doit le déchiffrer. La mise en oeuvre du procédé de déchiffrement par le dispositif B qui reçoit le message est un peu différente.

En effet, le calcul effectué dans le dispositif dans une instance de déchiffrement, pour retrouver le nombre m à partir du cryptogramme c devient le suivant :

$$m = \frac{\log_n(c^u \bmod n^2)}{\log_n(g^u \bmod n^2)} \bmod n.$$

On peut appliquer comme précédemment des variantes de calcul qui permettent d'accélérer le temps de traitement nécessaire.

Dans une première variante, on va ainsi précalculer une fois pour toutes la quantité :

$$\beta_{n,g} = \log_n(g^u \bmod n^2)^{-1} \bmod n$$

et la conserver secrètement en mémoire.

Lors d'une instance de déchiffrement d'un cryptogramme c reçu, le dispositif n'a plus qu'à effectuer le calcul suivant :

$$m = \log_n(c^u \bmod n^2)\ \beta_{n,g} \bmod n.$$

Dans une deuxième variante, on met en oeuvre le Théorème du Reste Chinois, en utilisant les fonctions $\log_p$ et $\log_q$ déjà vues pour effectuer le calcul de déchiffrement.

Lors d'une instance de cette variante du procédé de déchiffrement du cryptogramme c reçu, le dispositif effectue alors les calculs suivants :

1. $m_p = \log_p(c^u \bmod p^2)\log_p(g^u \bmod p^2)^{-1} \bmod p$
2. $m_q = \log_q(c^u \bmod q^2)\log_q(g^u \bmod q^2)^{-1} \bmod q$
3. $m = TRC(m_p, m_q, p, q)$.

Dans une troisième variante, on accélère encore le temps de traitement nécessaire au déchiffrement du cryptogramme c selon la deuxième variante, en précalculant les quantités suivantes :

$\beta_{p,g} = \log_p(g^u \bmod p^2)^{-1} \bmod p$

$\beta_{q,g} = \log_q(g^u \bmod q^2)^{-1} \bmod q$

et en les conservant de façon secrète dans le dispositif.

Lors d'une instance de calcul de cette troisième variante du procédé de déchiffrement du cryptogramme c reçu, le dispositif n'a alors plus qu'à effectuer les calculs suivants :

1. $m_p = \log_p(c^u \bmod p^2)\ \beta_{p,g} \bmod p$
2. $m_q = \log_q(c^u \bmod q^2)\ \beta_{q,g} \bmod q$
3. $m = TRC(m_p, m_q, p, q)$.

Dans un quatrième mode de réalisation de l'invention, le procédé de chiffrement et le procédé de déchiffrement sont tels qu'ils présentent la particularité d'être des permutations sur le groupe des entiers modulo n^2. En d'autres termes, si le message m s'exprime sur k bits, le cryptogramme c obtenu en appliquant le procédé de chiffrement sur m et la signature s obtenue en appliquant le procédé de déchiffrement sur m sont aussi sur k bits.

Cette particularité confère au procédé cryptographique la propriété supplémentaire de pouvoir

être utilisé aussi bien en chiffrement/déchiffrement qu'en génération/vérification de signature. Dans ce cas, le procédé de déchiffrement est employé comme procédé de génération de signature et le procédé de chiffrement comme procédé de vérification de signature.

Dans ce quatrième mode de réalisation, le procédé de génération des clés publique et privée est le même que celui du premier mode de réalisation de l'invention : $K=(n,g)$ et $K'=(p,q,\lambda(n))$ ou $K'=(p,q)$.

Si le dispositif A veut envoyer un message m chiffré au dispositif B, il se procure la clé publique (n,g) de ce dernier, puis dans une instance du procédé de chiffrement, effectue alors les calculs suivants, appliqué au nombre m, $0 \leq m < n^2$:

1. $m_1 = m \bmod n$
2. $m_2 = (m-m1)/n$ (division euclidienne)
3. $c = g^{m1}\, m_2^{\,n} \bmod n^2$.

C'est ce cryptogramme c qui est envoyé au dispositif B.

Ce dernier doit donc lui appliquer le procédé de déchiffrement correspondant, pour retrouver m_1, m_2 et finalement m. Ce procédé de déchiffrement selon le quatrième mode de réalisation de l'invention consiste à effectuer les calculs suivants :

1. $m_1 = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$.
2. $w = cg^{-m1} \bmod n$.
3. $m_2 = w^{1/n \bmod \lambda(n)} \bmod n$.
4. $m = m_1 + nm_2$.

Comme précédemment, des variantes du procédé de déchiffrement selon ce quatrième mode de réalisation de l'invention sont applicables, qui permettent de réduire le temps de traitement nécessaire pour déchiffrer un message donné. Elles sont intéressantes lorsque le dispositif a un grand nombre de cryptogrammes à déchiffrer.

Une première variante consiste à précalculer les quantités suivantes :

$\alpha_{n,g}=\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$ et

$\gamma_n = 1/n \bmod \lambda(n)$

que le dispositif B calcule une fois pour toutes et conserve secrètes en mémoire.

A chaque nouvelle instance de déchiffrement d'un cryptogramme c reçu selon cette première variante, le dispositif B n'a plus qu'à effectuer les calculs suivants :

1. $m_1=\log_n(c^{\lambda(n)} \bmod n^2)\ \alpha_{n,g} \bmod n$.
2. $w=cg^{-m1} \bmod n$.
3. $m_2=w^{\gamma n} \bmod n$.
4. $m = m_1 + nm_2$.

Dans une deuxième variante de la mise en oeuvre du procédé de déchiffrement selon le quatrième mode de réalisation, on utilise le Théorème du Reste Chinois.

Le dispositif qui veut déchiffrer un cryptogramme c selon cette deuxième variante effectue alors les calculs successifs suivants :

1. $m_{1,p}=\log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$
2. $w_p=cg^{-m1,p} \bmod p$
3. $m_{2,p}=w_p^{\,1/q \bmod p-1} \bmod p$
4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2)\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

5. $w_q = c g^{-m1,q} \bmod q$
6. $m_{2,q} = w_q^{1/p \bmod q-1} \bmod q$
7. $m_1 = TRC(m_{1,p}, m_{2,p}, p, q)$.
8. $m_2 = TRC(m_{1,q}, m_{2,q}, p, q)$.
9. $m = m_1 + pqm_2$.

Dans une troisième variante, pour améliorer encore le temps de traitement du déchiffrement de cette deuxième variante, le dispositif B peut précalculer une fois pour toutes les quantités suivantes :

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p = 1/q \bmod p-1$

$\gamma_q = 1/p \bmod q-1$

et les conserver secrètes en mémoire.

Le dispositif qui veut déchiffrer un cryptogramme c selon cette troisième variante n'a plus qu'à effectuer les calculs suivants:

1. $m_{1,p} = \log_p(c^{p-1} \bmod p^2)\ \alpha_{p,g} \bmod p$
2. $w_p = c g^{-m1,p} \bmod p$
3. $m_{2,p} = w_p^{\gamma p} \bmod p$
4. $m_{1,q} = \log_q(c^{q-1} \bmod q^2)\ \alpha_{q,g} \bmod q$
5. $w_q = c g^{-m1,q} \bmod q$
6. $m_{2,q} = w_q^{\gamma q} \bmod q$
7. $m_1 = TRC(m_{1,p}, m_{2,p}, p, q)$.
8. $m_2 = TRC(m_{1,q}, m_{2,q}, p, q)$.
9. $m = m_1 + pqm_2$.

Le quatrième mode de réalisation de l'invention qui vient d'être décrit permet de faire de la génération/

vérification de signature. Comme représenté sur l'organigramme de la figure 4, si le dispositif B doit générer une signature s d'un nombre m représentatif d'un message vers le dispositif A, il applique comme procédé de génération de la signature, le procédé de déchiffrement avec sa clé privée : $s=D_{K\cdot B}(m)$.

Le dispositif A qui reçoit la signature s et qui connaît le message m, vérifie que la signature est bonne en calculant la quantité v obtenue en appliquant le procédé de chiffrement sur la signature s avec la clé publique : $v=E_{K_B}(s)$. Si la signature est bonne, on a v=m.

Toutes les variantes de mise en oeuvre du procédé de déchiffrement de ce quatrième mode de réalisation qui permettent d'accélérer le temps de traitement sont aussi bien applicable en génération/vérification de signature.

L'invention qui vient d'être décrite est applicable dans tous les systèmes où l'on veut pouvoir chiffrer et/ou signer des messages. Elle permet d'élargir les possibilités d'adaptation aux différentes applications, selon que l'on recherche plus de sécurité, ou une vitesse de traitement accrue. A cet égard, on notera que le troisième mode de réalisation de l'invention, dont la complexité de calcul est seulement quadratique (fonction du carré de la taille de n) offre un réel avantage en terme de vitesse, dans la mesure où tous les procédés de l'état de la technique ont un ordre de complexité supérieur (fonction du cube de la taille de n). Un tel avantage intéresse plus particulièrement toutes les applications utilisant des dispositifs portables, tels les

cartes à puces et plus particulièrement les dispositifs à bas coûts.

Enfin, toute personne expérimentée dans la technique concernée par l'invention comprendra que des modifications dans la forme et/ou des détails peuvent être effectués sans sortir de l'esprit de l'invention. En particulier on peut chiffrer la signature, ou encore appliquer une fonction de hachage au message m avant de calculer sa signature.

REVENDICATIONS

1. Procédé cryptographique comprenant un procédé de génération de clés publique (K) et privée (K') dans un dispositif apte à échanger des messages sur au moins un canal de communication, la clé privée devant être conservée de façon secrète dans ledit dispositif et la clé publique devant être diffusée publiquement, le procédé de génération comprenant les étapes suivantes :

- sélection de deux nombres premiers p et q distincts, de taille voisine;
- calcul du nombre n égal au produit p.q;

caractérisé en ce que ledit procédé comprend en outre les étapes suivantes :

- calcul du plus petit commun multiple des nombres (p-1) et (q-1) : $\lambda(n)=PPCM(p-1, q-1)$
- détermination d'un nombre g , $0 \leq g < n^2$ qui vérifie les deux conditions suivantes :

a) g est inversible modulo n^2 et

b) $ord(g,n^2) = 0 \bmod n$,

la clé publique dudit dispositif étant formée par les paramètres n et g et sa clé privée étant formée par les paramètres p,q et $\lambda(n)$ ou par les paramètres p et q.

2. Procédé de génération selon la revendication 1, caractérisé en ce qu'il consiste à prendre g=2, si g vérifie les dites conditions a) et b).

3. Système de communication cryptographique à clés publique et privée générées selon la revendication 1 ou 2, comprenant un canal de communication (20) et des dispositifs communiquant (A, B), chaque dispositif comprenant au moins une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique (n_B, g_B) du deuxième dispositif (B) pour renseigner les paramètres n et g du procédé de chiffrement,
- calcul du cryptogramme $c = g^m \bmod n^2$,

ledit cryptogramme c étant ensuite transmis sur le canal de communication vers le deuxième dispositif.

4. Système selon la revendication 3 , caractérisé en ce que le dispositif mettant en oeuvre le procédé de chiffrement comprend en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

-effectue le tirage d'un nombre entier aléatoire r, puis

-calcule le cryptogramme c en effectuant le calcul de chiffrement suivant: $c = g^{m+nr} \bmod (n^2)$.

5. Système selon la revendication 3, caractérisé en ce que le dispositif mettant en oeuvre le procédé de

chiffrement comprend en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

-effectue le tirage d'un nombre entier aléatoire r, puis

-calcule le cryptogramme c en effectuant le calcul de chiffrement suivant: $c=g^m r^n \bmod(n^2)$.

6. Système selon l'une des revendications 3 à 5, caractérisé en ce que le deuxième dispositif (B) met en oeuvre un procédé de déchiffrement, pour déchiffrer ledit cryptogramme c, et qui comprend la réalisation du calcul

$$m= \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

où $\log_n(x)= \dfrac{x-1}{n}$.

7. Système selon la revendication 6, caractérisé en ce qu'un dispositif (B) mettant en oeuvre ledit procédé de déchiffrement, précalcule la quantité :

$$\alpha_{n,g}= \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

et la conserve secrètement.

8. Système selon la revendication 6, caractérisé en ce que dans une instance dudit procédé de déchiffrement un dispositif effectue les étapes de calcul suivantes, utilisant le Théorème du Reste Chinois TRC :

$$m_p=\log_p(c^{p-1} \bmod p^2).\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p.$$

$$m_q=\log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q.$$

$m=TRC(m_p,m_q,p,q)$, où $\log_p$ et $\log_q$ sont tels que

$$\log_i(x)= \frac{x-1}{i} .$$

9. Système selon la revendication 8, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule les quantités suivantes

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$ et

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$.

et les conserve secrètement.

10. Système de communication cryptographique à clés publique et privée générées selon la revendication 1 ou 2, comprenant un canal de communication (20) et des dispositifs communiquant (A,B), chaque dispositif comprenant une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n^2$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique $K_B=(n_B,g_B)$ du deuxième dispositif (B) pour renseigner les paramètres n et g du procédé de déchiffrement,
- et réalisation des calculs suivants :

1. $m_1 = m \bmod n$
2. $m_2 = (m - m1)/n$
3. $c = g^{m1}\, m_2^{\,n} \bmod n^2$.

ledit cryptogramme c étant transmis sur le canal de communication.

11. Système selon la revendication 10, caractérisé en ce que en ce que le deuxième dispositif (B) reçoit le cryptogramme c et met en oeuvre un procédé de déchiffrement, pour déchiffrer ledit cryptogramme qui comprend la réalisation des étapes suivantes de calcul :

1. $m_1=\log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$.
2. $w=cg^{-m1} \bmod n$.
3. $m_2=w^{1/n \bmod \lambda(n)} \bmod n$.
4. $m = m_1 + nm_2$.

12. Système selon la revendication 11, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement, précalcule les quantités suivantes :

$\alpha_{n,g}=\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$ et

$\gamma_n= 1/n \bmod \lambda(n)$

et les conserve secrètement.

13. Système selon la revendication 11, caractérisé en ce que dans une instance dudit procédé de déchiffrement, un dispositif effectue les étapes de calcul suivant, en utilisant le Théorème du Reste Chinois :

1. $m_{1,p}=\log_p(c^{p-1} \bmod p^2).\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$
2. $w_p=cg^{-m1,p} \bmod p$
3. $m_{2,p}=w_p^{1/q \bmod p-1} \bmod p$.
4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$
5. $w_q=cg^{-m1,q} \bmod q$
6. $m_{2,q}=w_q^{1/p \bmod q-1} \bmod q$
7. $m_1=TRC(m_{1,p},m_{2,p},p,q)$.
8. $m2=TRC(m_{1,q},m_{2,q},p,q)$.

9. $m = m_1 + pqm_2$, où $\log_p$ et $\log_q$ sont tels que

$$\log_i(x) = \frac{x-1}{i} .$$

14. Système selon la revendication 13, caractérisé en ce que dans une instance dudit procédé de déchiffrement, un dispositif précalcule les quantités suivantes :

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p = 1/q \bmod p-1$

$\gamma_q = 1/p \bmod q-1$

et les conserve secrètement.

15. Système selon l'une quelconque des revendications 11 à 14, dans lequel le procédé de déchiffrement est utilisé pour calculer la signature s d'un message m et le procédé de chiffrement est utilisé pour vérifier ladite signature.

16. Procédé cryptographique comprenant un procédé de génération de clés publique (K) et privée (K') dans un dispositif apte à échanger des messages sur au moins un canal de communication (20), la clé privée devant être conservée de façon secrète dans ledit dispositif et la clé publique devant être diffusée publiquement, procédé de génération caractérisé en ce qu'il comprend les étapes suivantes :

- sélection d'un nombre u et de deux nombres premiers p et q distincts, de taille voisine, tels que u divise (p-1) et divise (q-1);

- calcul du nombre n égal au produit p.q;

- calcul du plus petit commun multiple des nombres (p-1) et (q-1) : $\lambda(n)=PPCM(p-1, q-1)$

- détermination d'un nombre h , $0 \leq h < n^2$ qui vérifie les deux conditions suivantes :

a) h est inversible modulo n^2 et

b) $ord(h,n^2) = 0 \bmod n$,

- calcul du nombre $g=h^{\lambda(n)/u} \bmod n^2$,

la clé publique dudit dispositif étant formée par les paramètres n et g et sa clé privée étant formée par les paramètres p,q et u.

17. Procédé selon la revendication 16, caractérisé en ce qu'il consiste à choisir h=2, si les conditions a) et b) sont remplies.

18. Procédé selon la revendication 16, caractérisé en ce que u est le plus grand commun diviseur de (p-1), (q-1).

19. Procédé selon la revendication 16, caractérisé en ce que u est un nombre premier.

20. Système de communication cryptographique à clés publique et privée générées selon l'une des revendications 16 à 19, comprenant un canal de communication (20) et des dispositifs communiquant (A, B), chaque dispositif comprenant une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans

un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique $(n,g)_B$ du deuxième dispositif (B) pour renseigner les paramètres n et g du procédé de chiffrement,
- calcul du cryptogramme $c = g^m \bmod n^2$,

ledit cryptogramme c étant ensuite transmis sur le canal de communication vers le deuxième dispositif.

21. Système selon la revendication 20, caractérisé en ce que le dispositif mettant en oeuvre le procédé de chiffrement comprend en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

-effectue le tirage d'un nombre entier aléatoire r, puis

-calcule le cryptogramme c en effectuant le calcul de chiffrement suivant: $c = g^{m+nr} \bmod (n^2)$.

22. Système selon la revendication 20 ou 21, caractérisé en ce que le deuxième dispositif met en oeuvre un procédé de déchiffrement du cryptogramme reçu c, comprenant la réalisation du calcul suivant :

$$m = \log_n(c^u \bmod n^2).\log_n(g^u \bmod n^2)^{-1} \bmod n.$$

23. Procédé selon la revendication 22, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule la quantité :

$$\beta_{n,g} = \log_n(g^u \bmod n^2)^{-1} \bmod n$$

et la conserve secrètement .

24. Système selon la revendication 22, caractérisé en ce que dans une instance dudit procédé de déchiffrement, un dispositif effectue les étapes de calcul suivantes, en utilisant le Théorème du reste chinois :

1. $m_p = \log_p(c^u \bmod p^2).\log_p(g^u \bmod p^2)^{-1} \bmod p$.
2. $m_q = \log_q(c^u \bmod q^2).\log_q(g^u \bmod q^2)^{-1} \bmod q$.
3. $m = TRC(m_p, m_q, p, q)$, où $\log_p$ et $\log_q$ sont tels que

$$\log_i(x) = \frac{x-1}{i}.$$

25. Système selon la revendication 24, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule les quantités suivantes :

$\beta_{p,g} = \log_n(g^u \bmod p^2)^{-1} \bmod p$

$\beta_{q,g} = \log_n(g^u \bmod q^2)^{-1} \bmod q$

et les conserve secrètement.

Un objet de l'invention, est un procédé reposant sur d'autres propriétés, qui puisse s'appliquer aussi bien en chiffrement de messages qu'en génération de signatures.

Un objet de l'invention, est un procédé de cryptographie qui permette, dans certaines configurations, un temps de traitement plus rapide.

Telle que caractérisée, l'invention concerne un procédé cryptographique comprenant un procédé de génération de clés publique (K) et privée (K') dans un dispositif apte à échanger des messages sur au moins un canal de communication, la clé privée devant être conservée de façon secrète dans ledit dispositif et la clé publique devant être diffusée publiquement, le procédé de génération comprenant les étapes suivantes :

- sélection de deux nombres premiers p et q distincts, de taille voisine;
- calcul du nombre n égal au produit p.q;

caractérisé en ce que ledit procédé comprend en outre les étapes suivantes :

- calcul du plus petit commun multiple des nombres (p-1) et (q-1) : $\lambda(n)=PPCM(p-1, q-1)$
- détermination d'un nombre g , $0 \leq g < n^2$ qui vérifie les deux conditions suivantes :

a) g est inversible modulo n^2 et

b) $ord(g,n^2) = 0 \bmod n$,

la clé publique dudit dispositif étant formée par les paramètres n et g et sa clé privée étant formée par les paramètres p,q et $\lambda(n)$ ou par les paramètres p et q.

L'invention sera mieux comprise à la lecture de la description suivante , faite à titre indicatif et nullement limitatif de l'invention et en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma fonctionnel d'un système de communication cryptographique de type asymétrique;
- la figure 2 est un schéma fonctionnel d'un dispositif communiquant utilisé dans un système de communication cryptographique selon l'invention;
- la figure 3 est un organigramme d'une session de chiffrement/déchiffrement de messages utilisant le procédé cryptographique selon l'invention; et
- la figure 4 est un organigramme d'une session de génération/vérification de signature utilisant le procédé cryptographique selon l'invention.

Pour bien comprendre l'invention, il est nécessaire de faire quelques préliminaires mathématiques.

Dans la description, on utilise les notations mathématiques suivantes :

(1) Si a est un entier relatif et b un entier strictement positif, a mod b (a modulo b) est le résidu modulaire de a relativement à b et désigne l'unique entier strictement inférieur à b tel que b divise (a - a mod b).

(2) (Z/bZ) désigne l'ensemble des résidus modulo b et forme un groupe pour l'addition modulaire .

(3) $(Z/bZ)^*$ désigne l'ensemble des entiers inversibles modulo b et forme un groupe pour la multiplication modulaire.

notera que dans le RSA, c'est le message m qui est élevé à la puissance alors que dans l'invention, le message m est utilisé comme exposant.

Le dispositif B qui reçoit le message chiffré, c'est à dire le cryptogramme c, met alors en oeuvre un procédé de déchiffrement selon l'invention avec les paramètres de sa clé privée. Ce procédé de déchiffrement comprend le calcul suivant :

- calcul du nombre m tel que

$$m = \frac{\log_n(c^{\lambda(n)} \bmod n^2)}{\log_n(g^{\lambda(n)} \bmod n^2)} \bmod n$$

où

$$\log_n(x) = \frac{x-1}{n} .$$

Si g=2, on voit que le calcul d'élévation de g à la puissance est facilité. On prendra donc de préférence g=2, toutes les fois où ce sera possible. En d'autres termes, le procédé de génération des clés commencera par essayer si g=2 remplit les conditions a) et b).

Différentes variantes de calcul du procédé de déchiffrement peuvent être mises en oeuvre, qui permettent, lorsque le dispositif doit déchiffrer un grand nombre de cryptogrammes, de précalculer certaines quantités et de les conserver de façon secrète dans le dispositif. Une contrepartie est que la zone mémoire secrète (zone 120 sur la figure 2) du dispositif doit être plus étendue, puisqu'elle doit alors contenir des paramètres supplémentaires en plus des paramètres p et q. Ceci n'est pas sans influencer le choix de mise en oeuvre d'une variante ou d'une autre. En effet, la réalisation

d'une zone de mémoire sécurisée est coûteuse, et donc de capacité (mémoire) généralement limitée, notamment dans les dispositifs dits à bas côuts (par exemple, certains types de cartes à puce).

Dans une première variante de mise en oeuvre du procédé de déchiffrement, on prévoit que le dispositif, B en l'occurrence, précalcule une fois pour toutes la quantité :

$$\alpha_{n,g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

et la conserve secrète en mémoire.

Ainsi, on réduit d'autant le temps nécessaire au déchiffrement de chacun des messages reçus par le dispositif. En effet, lorsque que le dispositif B exécute une instance de cette variante du procédé de déchiffrement, il ne lui reste plus qu'à calculer :

$$m = \log_n(c^{\lambda(n)} \bmod n^2)\ \alpha_{n,g} \bmod n.$$

Dans une deuxième variante de mise en oeuvre du procédé de déchiffrement selon l'invention, on prévoit d'utiliser le Théorème du Reste Chinois, pour une meilleure efficacité (rapidité du calcul).

Dans une instance de cette deuxième variante du procédé de déchiffrement, le dispositif effectue les calculs (de déchiffrement) suivants :

1 $m_p = \log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

2 $m_q = \log_q(c^{q-1} \bmod q^2)\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

3 $m = TRC(m_p, m_q, p, q)$,

où

$$\log_p(x) = \frac{x-1}{p} \qquad \text{et}$$

REVENDICATIONS

1. Procédé cryptographique comprenant un procédé de génération de clés publique (K) et privée (K') dans un dispositif apte à échanger des messages sur au moins un canal de communication, la clé privée devant être conservée de façon secrète dans ledit dispositif et la clé publique devant être diffusée publiquement, le procédé de génération comprenant les étapes suivantes :

- sélection de deux nombres premiers p et q distincts, de taille voisine;
- calcul du nombre n égal au produit p.q;

caractérisé en ce que ledit procédé comprend en outre les étapes suivantes :

- calcul du plus petit commun multiple des nombres (p-1) et (q-1) : $\lambda(n)=PPCM(p-1, q-1)$
- détermination d'un nombre g , $0 \leq g < n^2$ qui vérifie les deux conditions suivantes :

a) g est inversible modulo n^2 et

b) $ord(g,n^2) = 0 \bmod n$,

la clé publique dudit dispositif étant formée par les paramètres n et g et sa clé privée étant formée par les paramètres p,q et $\lambda(n)$ ou par les paramètres p et q.

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste à prendre g=2, si g vérifie les dites conditions a) et b).

3. Système de communication cryptographique à clés publique et privée générées suivant un procédé selon la revendication 1 ou 2, comprenant un canal de communication (20) et des dispositifs communiquant (A, B), chaque dispositif comprenant au moins une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique (n_B, g_B) du deuxième dispositif (B) pour renseigner les paramètres n et g du procédé de chiffrement,
- calcul du cryptogramme $c = g^m \bmod n^2$,

ledit cryptogramme c étant ensuite transmis sur le canal de communication vers le deuxième dispositif.

4. Système selon la revendication 3 , caractérisé en ce que le dispositif mettant en oeuvre le procédé de chiffrement comprend en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

-effectue le tirage d'un nombre entier aléatoire r, puis

-calcule le cryptogramme c en effectuant le calcul de chiffrement suivant: $c = g^{m+nr} \bmod (n^2)$.

5. Système selon la revendication 3, caractérisé en ce que le dispositif mettant en oeuvre le procédé de

9. Système selon la revendication 8, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule les quantités suivantes

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$ et

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$.

et les conserve secrètement.

10. Système de communication cryptographique à clés publique et privée générées suivant un procédé selon la revendication 1 ou 2, comprenant un canal de communication (20) et des dispositifs communiquant (A,B), chaque dispositif comprenant une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n^2$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique $K_B=(n_B, g_B)$ du deuxième dispositif (B) pour renseigner les paramètres n et g du procédé de déchiffrement,
- et réalisation des calculs suivants :

1. $m_1 = m \bmod n$
2. $m_2 = (m - m1)/n$
3. $c = g^{m1}\, m_2^{\,n} \bmod n^2$.

ledit cryptogramme c étant transmis sur le canal de communication.

un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique $(n,g)_B$ du deuxième dispositif (B) pour renseigner les paramètres n et g du procédé de chiffrement,
- calcul du cryptogramme $c = g^m \bmod n^2$,

ledit cryptogramme c étant ensuite transmis sur le canal de communication vers le deuxième dispositif.

21. Système selon la revendication 20, caractérisé en ce que le dispositif mettant en oeuvre le procédé de chiffrement comprend en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

-effectue le tirage d'un nombre entier aléatoire r, puis

-calcule le cryptogramme c en effectuant le calcul de chiffrement suivant: $c = g^{m+nr} \bmod (n^2)$.

22. Système selon la revendication 20 ou 21, caractérisé en ce que le deuxième dispositif met en oeuvre un procédé de déchiffrement du cryptogramme reçu c, comprenant la réalisation du calcul suivant :

$$m = \log_n(c^u \bmod n^2).\log_n(g^u \bmod n^2)^{-1} \bmod n.$$

23. Système selon la revendication 22, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule la quantité :

$$\beta_{n,g} = \log_n(g^u \bmod n^2)^{-1} \bmod n$$

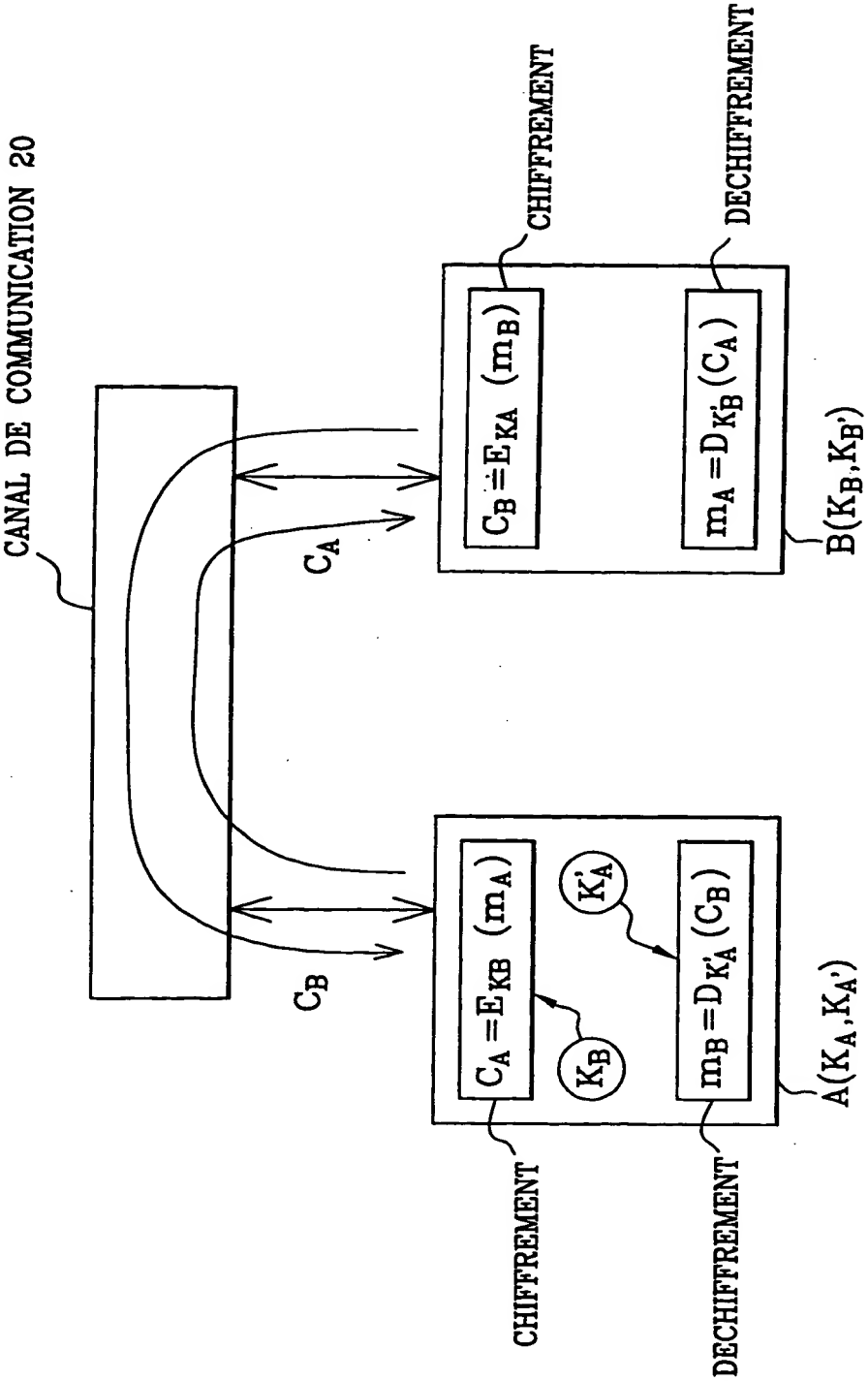
CANAL DE COMMUNICATION 20
C_A
C_B
$C_B = E_{KA}(m_B)$
CHIFFREMENT
$m_A = D_{K'B}(C_A)$
DECHIFFREMENT
$B(K_B, K_{B'})$
$C_A = E_{KB}(m_A)$
K_B
K'_A
$m_B = D_{K'A}(C_B)$
CHIFFREMENT
DECHIFFREMENT
$A(K_A, K_{A'})$

FIG.1

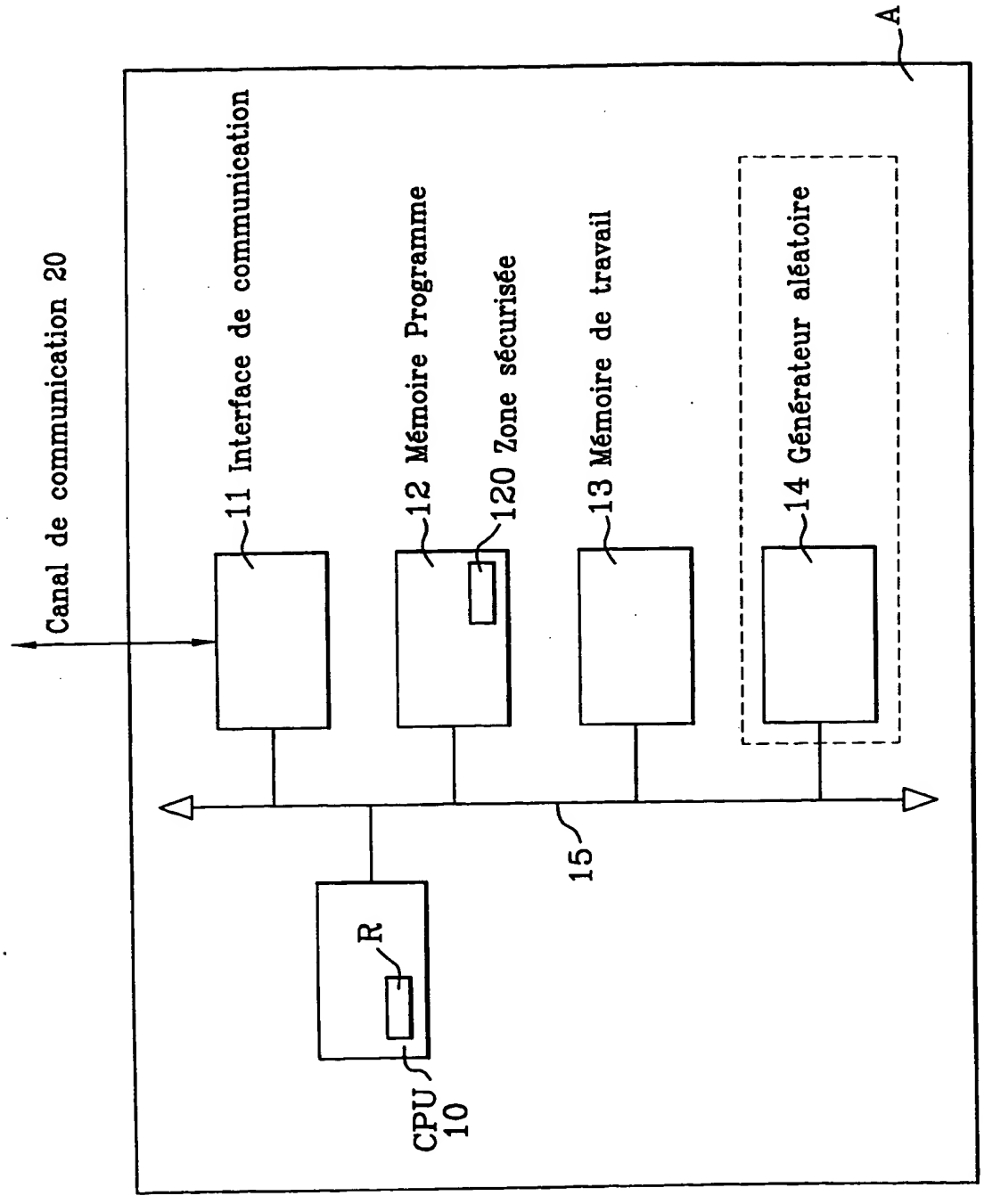
A
Canal de communication 20
11 Interface de communication
12 Mémoire Programme
120 Zone sécurisée
13 Mémoire de travail
14 Générateur aléatoire
15
R
CPU
10

FIG.2

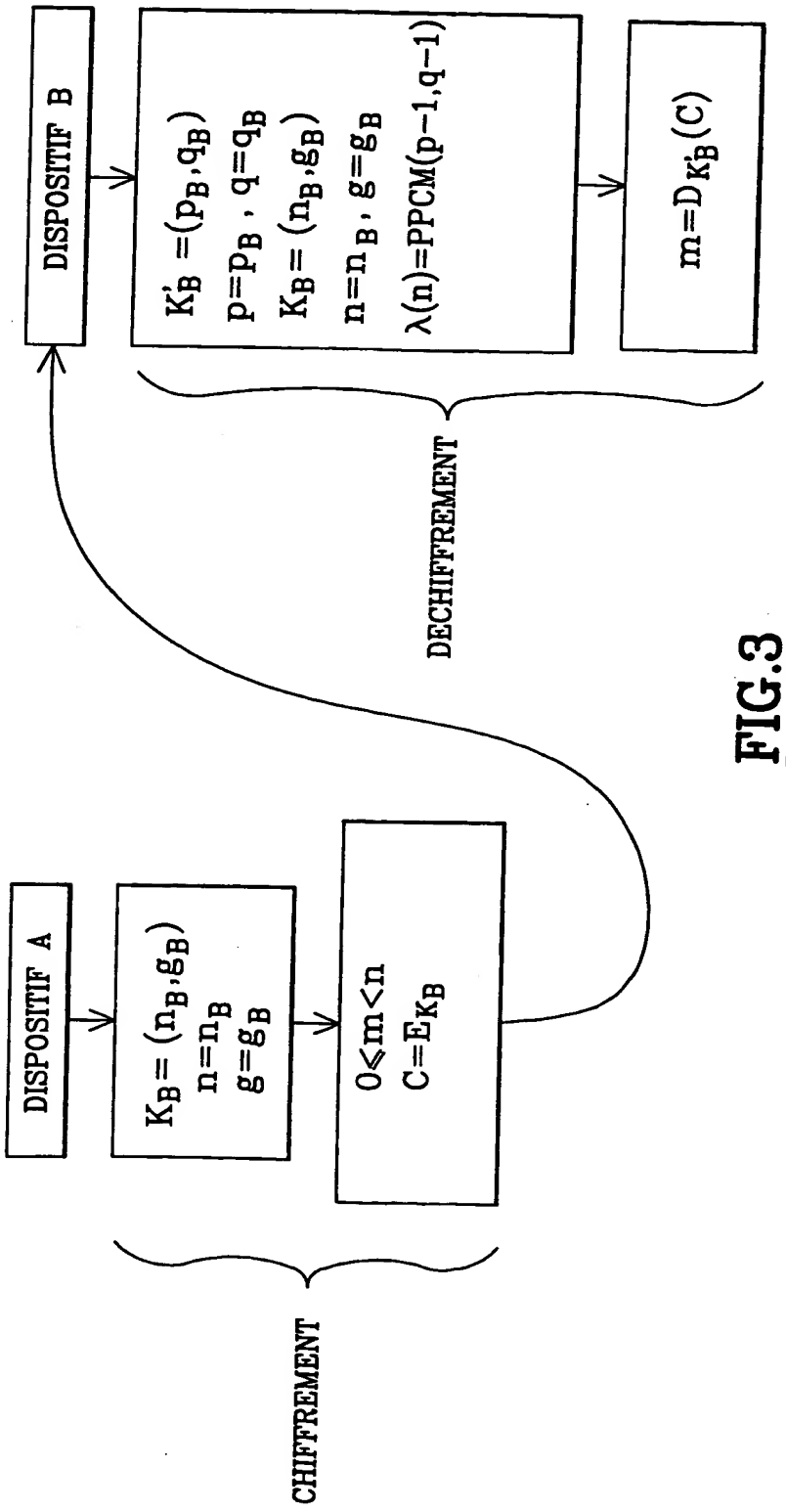
DISPOSITIF A
$K_B = (n_B, g_B)$
$n = n_B$
$g = g_B$
$0 \leqslant m < n$
$C = E_{K_B}$
CHIFFREMENT
DISPOSITIF B
$K'_B = (p_B, q_B)$
$p = p_B$, $q = q_B$
$K_B = (n_B, g_B)$
$n = n_B$, $g = g_B$
$\lambda(n) = PPCM(p-1, q-1)$
$m = D_{K'_B}(C)$
DECHIFFREMENT

FIG.3

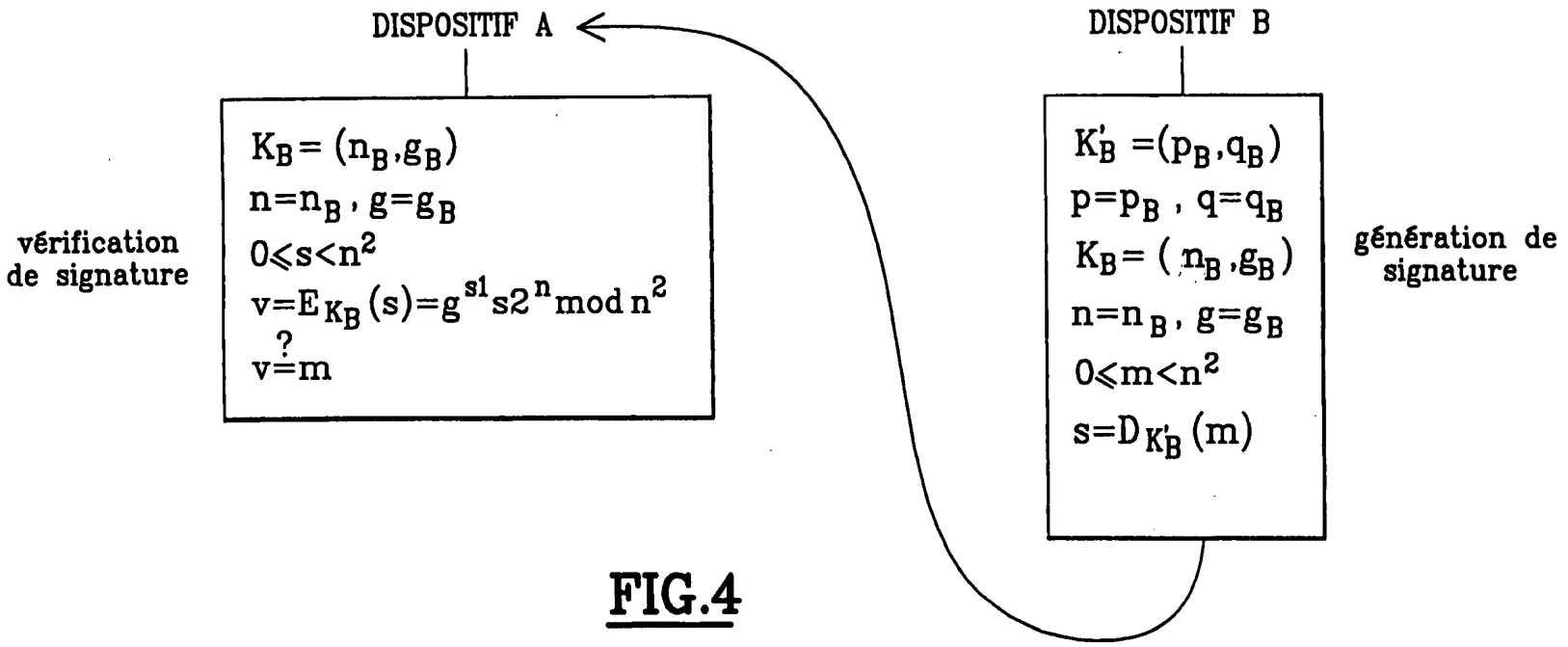
DISPOSITIF A
DISPOSITIF B
$K_B = (n_B, g_B)$
$n = n_B$, $g = g_B$
$0 \leqslant s < n^2$
$v = E_{K_B}(s) = g^{s1} s2^n \bmod n^2$
$v \stackrel{?}{=} m$
vérification de signature
$K'_B = (p_B, q_B)$
$p = p_B$, $q = q_B$
$K_B = (n_B, g_B)$
$n = n_B$, $g = g_B$
$0 \leqslant m < n^2$
$s = D_{K'_B}(m)$
génération de signature

FIG.4

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☑ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.